ISSN 1064-5624, Doklady Mathematics, 2018, Vol. 98, No. 1, pp. 341–343. © Pleiades Publishing, Ltd., 2018.
Original Russian Text © P.E. Alaev, V.L. Selivanov, 2018, published in Doklady Akademii Nauk, 2018, Vol. 481, No. 4.

MATHEMATICS

Polynomial Computability of Fields of Algebraic Numbers[1]

P. E. Alaev[a,b,*] and V. L. Selivanov[c,d,]**

Received March 19, 2018

Abstract— We prove that the field of complex algebraic numbers and the ordered field of real algebraic numbers have isomorphic presentations computable in polynomial time. For these presentations, new algorithms are found for evaluation of polynomials and solving equations of one unknown. It is proved that all best known presentations for these fields produce polynomially computable structures or quotient-structures such that there exists an isomorphism between them polynomially computable in both directions.

DOI: 10.1134/S1064562418050137

1. EXISTENCE OF A POLYNOMIAL PRESENTATION

Let Σ denote a finite alphabet everywhere in the paper. By Σ^* we denote the set of all words in the alphabet Σ. A structure (model, or algebraic system) $\mathfrak{A}$ consists of a non-empty set A, the universe of the structure, and relations, operations and constants defined on it. A set of symbols for these objects is called the language (or signature) of the structure.

In the present paper, we consider structures whose universe is a subset of Σ^* for some Σ. A structure $\mathfrak{A}$ of a finite language is computable if its universe A and all its relations and operations are computable, i.e., can be defined with some algorithms. We say that a structure $\mathfrak{A}$ has a computable presentation (is constructivizable) if it is isomorphic to a computable structure.

The theory of computable structures arose long ago, and now it is one of the main research directions in the general computability theory. Significant contributions to its development were made by A.I. Maltsev, Yu.L. Ershov, S.S. Goncharov, and many others domestic and foreign mathematicians. One of the first papers in this area was the article [1], where the following fact was proved: if a field $\mathfrak{F}$ has a computable presentation then this also holds for its algebraic closure. Let $\mathbb{C}_{alg}$ denote the set of all complex algebraic numbers, and let $\mathbb{R}_{alg} = \mathbb{C}_{alg} \cap \mathbb{R}$ denote the set of all real algebraic numbers, i.e., numbers that are roots of a non-zero polynomial with integer coefficients. The field of rational numbers $(\mathbb{Q},+,\times)$ has a computable presentations, hence, this also holds for the field $\mathfrak{A}^C = (\mathbb{C}_{alg},+,\times)$.

It is proved in [2] that if an ordered field $\mathfrak{F} = (F,\leq,+,\times)$ has a computable presentation then it also holds for its real closure. Since the field $\mathfrak{A}^R = (\mathbb{R}_{alg},\leq,+,\times)$ is the real closure of the ordered field $(\mathbb{Q},\leq,+,\times)$, it also has a computable presentation. A general proof of these facts can be found in the book [3], which also includes foundation of the theory of computable structures.

The present paper is devoted to investigating structures computable in polynomial time. We use multitape Turing machines [4] as a basic computational device. Let $A \subseteq (\Sigma^*)^n$ and $f: A \to \Sigma^*$. We say that f is computable in polynomial time (p-computable) if there exists a k-tape Turing machine, $k \geq n+1$, that takes a set of words $x_1, \ldots, x_n = \overline{x} \in A$ as an input and returns the word $f(\overline{x})$ as the result in no more than $c|\overline{x}|^m$ steps for $|\overline{x}| \neq 0$, where c, m are fixed constants and $|\overline{x}| = \max_{i\leq n}\{|x_i|\}$. We can consider such functions as "quickly computable." A set $A \subseteq (\Sigma^*)^n$ is p-computable if $\chi_A: (\Sigma^*)^n \to \{0,1\}$ is.

A structure $\mathfrak{A}$ of a finite language is computable in polynomial time (p-computable) if there is a finite alphabet Σ such that $A \subseteq \Sigma^*$ and A itself and all its relations and operations are p-computable. We say

[1] The article was translated by the authors.

[a] *Sobolev Institute of Mathematics of the Siberian Branch of the Russian Academy of Sciences, Novosibirsk, 630090 Russia*
[b] *Novosibirsk State University, Novosibirsk, 630090 Russia*
[c] *Ershov Institute of Informatics System of the Siberian Branch of the Russian Academy of Sciences, Novosibirsk, Russia*
[d] *Kazan Federal University, Kazan, 420008 Republic of Tatarstan, Russia*
**e-mail: alaev@math.nsc.ru*
***e-mail: vseliv@iis.nsk.su*